

REMARKS

In the subject action, claims 1-31 were rejected. In response, Applicant respectfully traverses the Examiner's rejections.

Claims 1-8, 10-18, 20-29 and 31 were rejected under 35 USC 103(a) as being unpatentable over Wright (USP 6,052,486) and further in view of Nakamura (USP 5,159, 633) and Coppersmith (USP 6,192,129).

Claim 1 recites, among other things,

generating in real time a second deciphering round key based on said generated first deciphering round key while said incremental deciphering for a first round is being performed; and
incrementally deciphering the partially deciphered text for a second round using the real time generated second deciphering round key.

Wright teaches of encryption and decryption using a stream cipher (see element 120 of Figure 3, and the corresponding description in column 5, lines 5-13). Nakamura teaches of encryption and decryption using an EX-OR technique (see e.g. elements 110 and 210 of Fig. 1A and 1B, and the corresponding descriptions in column 4, lines 40-45 and col. 5, lines 5-10). Coppersmith teaches of encryption and decryption using a block cipher (see e.g. Abstract), involving multiple rounds of deciphering, using multiple deciphering round keys, for a block of ciphered text. Fig. 3A and 3B illustrate how Coppersmith's block cipher works. The deciphering operations are illustrated in Fig. 4a and 4b.

Under Wright and Nakamura, for each data bit/byte deciphered, there is only one round of deciphering, using a single deciphering key. For each data bit/byte deciphered, there are no deciphering rounds or multiple deciphering round keys to speak of, regardless of how the deciphering round keys are generated. There is no application of any of Coppersmith's multiple deciphering round practices and/or teachings to Wright and Nakamura. It would fundamentally destroy the operation principles of a stream and a XOR cipher.

While under Wright the deciphering key for the next data bit/byte is in part dependent on the deciphering of the immediately preceding data bit/byte, it is integrally generated from the deciphering of the immediately preceding data bit/byte, and not generated in parallel with the deciphering of the immediately preceding data bit/byte. Thus, the combination of Wright and Nakamura with Coppersmith still fails to suggest at least the above enumerated recitations, that is, the parallel generation of a second deciphering round key to be applied to the continued incremental deciphering of a ciphered data block, using a first deciphering round key, while the ciphered data block is incrementally (partially) deciphered using the first deciphering round key.

Accordingly, the combination fails to teach or suggest at least the above enumerated recitations. Therefore, claim 1 is not obvious, and patentable over Wright, Nakamura and Coppersmith combined.

Each of claims 10 and 21 contains in substance the same recitation of claim 1. Accordingly, claims 10 and 21 are patentable over Wright, Nakamura and Coppersmith combined.

Claims 2-8, 11-18, 20, 22-29 and 31 depend on claims 1, 10 and 21, incorporating their limitations respectively. Accordingly, for at least the same reasons, claims 2-8, 11-18, 20, 22-29 and 31 are patentable over Wright, Nakamura and Coppersmith combined.


Claims 9, 19 and 30 were rejected in view of Wright, Nakamura and Adler. Adler does not remedy the above discussed deficiencies of Wright and Nakamura. Accordingly, claims 1, 10 and 21 remain patentable over Wright and Nakamura, even when combined with Adler. Claims 9, 19 and 30 depend on claims 1, 10 and 21, incorporating their limitations respectively. Thus, for at least the same reasons, claims 9, 19 and 30 are patentable over Wright and Nakamura, and Adler combined.

In view of the foregoing, Applicants submit claims 1-31 are in condition of allowance. Issuance of the Notice of Allowance is respectfully requested.

The Commissioner is hereby authorized to charge shortages or credit overpayments of fees to Deposit Account No. 500393.

Respectfully submitted,
SCHWABE, WILLIAMSON & WYATT, P.C.

Dated: 7/12/08


Aloysius T.C. AuYeung
Reg. No. 35,432

Pacwest Center, Suite 1900
1211 SW Fifth Avenue
Portland, Oregon 97204
Telephone: 503-222-9981